FOR PUBLICATION

ATTORNEY FOR APPELLANT:

ROBERT W. HAMMERLE
JOSEPH M. CLEARY
Hammerle & Cleary
Indianapolis, Indiana

ATTORNEYS FOR APPELLEE:

STEVE CARTER
Attorney General of Indiana

IAN MCLEAN
Deputy Attorney General
Indianapolis, Indiana

IN THE
COURT OF APPEALS OF INDIANA

BRIAN MEHRING,	)	
	)	
Appellant-Defendant,	)	
	)	
vs.	)	No. 49A05-0706-CR-337
	)	
STATE OF INDIANA,	)	
	)	
Appellee-.	)	

APPEAL FROM THE MARION SUPERIOR COURT
The Honorable Robert R. Altice, Jr., Judge and
The Honorable Amy Barbar, Magistrate
Cause No. 49G02-0611-FC-213393

April 15, 2008

OPINION - FOR PUBLICATION

FRIEDLANDER, Judge

In this interlocutory appeal, Brian Mehring appeals the trial court's denial of his motion to suppress evidence in a case in which he was charged with four counts of Child Exploitation,[1] each a class C felony, and nine counts of Possession of Child Pornography,[2] each a class D felony. Mehring presents the following restated issue for review: Did the trial court err in denying Mehring's motion to suppress?

We affirm.

On May 4, 2005, FBI Agent Michael Gordon, who was working in the FBI's New Orleans office, entered a "file sharing network" on the internet known as "LimeWire peer to peer." *Appellant's Appendix* at 39. The facts of what Agent Gordon discovered on this file sharing network and the subsequent acts of the police investigation are best described in the search warrant affidavit filled out by Detective Kurt Spivey of the Indianapolis Police Department's "Core Vice Unit", *id.*, when he applied for a warrant to search Mehring's apartment and computer:

> . . . [Agent Gordon] located several digital images which were available and were downloaded from IP Address 65.29.77.5. The downloads contained the images of prepubescent females in a state of nudity, with the focus on the genital area. The images appear to be produced for sexual arousal. After identifying the images as illegal child pornography, he tracked this IP Address and identified the Internet Service Provider (ISP). He sent an administrative subpoena to Bright house [sic] Networks, Inc., requesting information for the before mentioned IP Address. The subpoena return indicated the IP Address in question belonged to Brian Mehring at 732 Lockfield Court Apt B, Indianapolis, Indiana, at the specific date and time of the download. On 06-27-05, FBI Agent Michael Gordon reassigned this case to FBI Agent Dorian Deligeorges of the FBI Indianapolis Field Office. On 10-04-05 Agent Deligeorges requested assistance from the Indianapolis

[1] Ind. Code Ann. § 35-42-4-4(b) (West, PREMISE through 2007 1st Regular Sess.).

[2] I.C. § 35-42-4-4(c).

> Police Department to pursue a local level investigation and/or prosecution. On 10-05-05, I [Detective Spivey] approached the residence and found it to be vacant. Further investigation showed that Brian Mehring had relocated to 896 Blake Street, Apartment "B" which is also in the Lockfield Gardens Apartment Complex. On 03-09-06 at 23:45 hours, Patrolman Terry Snyder of the Indianapolis Police Department approached apartment 896-B, which had the name "Mehring" on the mailbox. He then knocked on the door under the ruse of a fake 911 call and positively identified Brian Mehring by name and date of birth. Through my training and experience, I know collectors of Child Pornography to go to great lengths to store, preserve and protect their collections. This is due to the illegal nature of said collection, contributing to the difficulty in obtaining and/or pornography, [sic] again contributing to the preservation of these collections for long periods of time. It is believed that the personal computer of Brian Mehring possesses the illegal child pornography received by Agent Gordon. It is also probable that this computer is located at 896 Blake Street, Apartment "B".

Id. at 39-40.

On March 23, 2006, Detective Spivey used this information to apply for and obtain a search warrant of Mehring's residence for "[a]ny and all materials, supplies, devices used to produce, transport, develop, promote, store, distribute or display child pornography and/or child exploitation." *Id.* at 38. The police executed the search warrant that same day and recovered several computers, computer towers, hard drives, and digital media, some of which contained images of child pornography.

Based on the evidence obtained from the search warrant, the State charged Mehring with four counts of class C felony child exploitation and nine counts of class D felony possession of child pornography. In January 2007, Mehring filed a motion to suppress, arguing that the search of his residence was unreasonable and unconstitutional under the Fourth Amendment to the United States Constitution and article 1, section 11 of the Indiana Constitution. Mehring argued that the search warrant should not have been

issued because it was based on stale information. Mehring also argued that there was a lack of probable cause supporting the warrant because the search warrant affidavit did not allege facts that would establish a fair probability that evidence of a crime would be found at his residence. In regard to the probable cause argument, Mehring argued, among other things, that there were insufficient facts from which the magistrate could determine that the images obtained from Mehring's IP address were illegal child pornography or determine that the Brian Mehring at the 896 Blake Street address was the same Brian Mehring as at the 732 Lockfield Court address.

On April 24, 2007, the trial court issued an order denying Mehring's motion to suppress. The trial court's order, which concluded that the warrant was supported by probable cause[3] and that the information in the warrant was not stale, provided, in relevant part:

* * * * *

> 5. The affidavit told the magistrate that several "digital images" were downloaded from a particular computer IP address in a file sharing network. The downloads were described as "images of prepubescent females in a state of nudity, with the focus on the genital area. The images appear to be produced for sexual arousal." In a practical, non-technical point of view, any reasonable person would interpret this to mean that there were photographs of naked pre-teen girls and their genitals available from this IP address. The magistrate could reasonably conclude that child pornography may be located at the place and in the storage of the computer with that IP address. Further, the physical address of the location of the computer was sufficiently corroborated by the affiant, through the name on the mailbox and ruse of Officer Snyder to verify the residence as that of Brian Mehring.

[3] Mehring contends that the trial court's order only addressed his staleness argument and did not address his probable cause argument. Based on his arguments and the trial court's order, we disagree.

6. The fact that the images were downloaded ten months before the warrant issued does not necessarily vitiate the probable cause. While information given to the magistrate must be timely, timeliness is not determined by a specific measure of time. " . . .(O)ur courts have not established a precise rule as to how much time may elapse between the obtaining of the facts upon which the search warrant is based and the issuance of the warrant (*cite omitted*) . . . Accordingly, probable cause is not determined by merely counting the number of days between the occurrence of the facts relied upon and the warrant's issuance . . . Instead, the staleness of the information must be judged by the facts and circumstances of each case." *Breitweiser,* at 499.

7. The federal courts have dealt extensively with the issue of staleness and computer transmissions of pornography. The very nature and characteristics of computer storage are such that one cannot make comparisons with those cases involving easily movable and destroyable items such as drugs. While the legal principles remain the same, the circumstances are distinguishable. In *U.S. v. Lacy*, 119 F.3d 742 (9th Circuit, 1997), the Court found that evidence that Lacy downloaded two sexually explicit images of minors provided "sufficient evidence Lacy actually received computerized visual depictions of child pornography." *Id.*, at 754. The information relied upon in the Lacy affidavit was ten months old. The Court found that because the agent, in the affidavit, explained that collectors and distributors of child pornography value their sexually explicit materials highly and rarely if ever dispose of their material, the magistrate had "good reason to believe the computerized visual depictions downloaded by Lacy would be present in his apartment when the search was conducted ten months later." *Id.* [*a*]*t* 746. In *U.S. v. Newsom*, 402 F.3d 780 (7th Circuit 2005), the computer information was a year old. While there was additional information of a recent video, the Court acknowledged the availability of immense amounts of storage space for long periods of time provided by computers. "Information a year old is not necessarily stale as a matter of law, especially where child pornography is concerned." *Supra, at* 783.

8. In this case, the affiant explained that based upon his training and experience, he knows "collectors of Child Pornography to go to great lengths to store, preserve and protect their collections" due to the illegal nature of the collection and difficulty in obtaining it. It was clear from the context of the affidavit that the police believed Mehring probably still had the ten month old image or similar images on his computer. The Court declines to define what number of pictures makes someone a "collector". The Court in *U.S. v. Lamb*, *supra*, held that "the magistrate need not have

> concluded that defendant was a pedophile, preferential child molester, or child pornography collector in order to decide that evidence of crime would likely be found at defendant's house in September of 1995. *The nature and characteristics of computer storage systems leads the court to believe that five and a half months is not so long that one would expect a computer file to be erased*." [*U.S. v. Lamb*, 945 F.Supp.] [a]t 461 (emphasis added).
>
> 9. The issuing magistrate herein had a substantial basis for concluding that evidence of a crime, that is possession of child pornography, would likely be found in [Mehring's] computer and/or at [Mehring's] home.

Appellant's Appendix at 55-57. Upon Mehring's request, the trial court certified its order for interlocutory appeal. We accepted jurisdiction of the appeal on May 7, 2007, pursuant to Ind. Appellate Rule 14(B).

Mehring argues that the trial court erred in denying his motion to suppress all evidence collected from his residence pursuant to the search warrant because the search of his residence was unreasonable and unconstitutional under the Fourth Amendment to the United States Constitution and article 1, section 11 of the Indiana Constitution. Specifically, Mehring contends that the warrant was not supported by probable cause because the information contained in the warrant was stale and because there were no facts from which the magistrate could conclude that the Brian Mehring at the 896 Blake Street address was the same Brian Mehring who lived at the 732 Lockfield Court address or that Mehring still had the computer or the images downloaded by the FBI agent in May 2005 on his computer when the warrant was issued and executed in March 2006.

Initially, we note that our review of a trial court's denial of a motion to suppress is similar to other sufficiency matters. *Litchfield v. State*, 824 N.E.2d 356 (Ind. 2005). That is, the record must disclose substantial evidence of probative value that supports the trial

court's decision. *Id.* We do not reweigh the evidence and we consider conflicting evidence most favorably to the trial court's ruling. *Id.*

The Fourth Amendment to the United States Constitution and article 1, section 11 of the Indiana Constitution both require probable cause for the issuance of a search warrant. *Breitweiser v. State*, 704 N.E.2d 496 (Ind. Ct. App. 1999). Probable cause is "a fluid concept incapable of precise definition . . . [and] is to be decided based on the facts of each case." *Figert v. State*, 686 N.E.2d 827, 830 (Ind. 1997). In deciding whether to issue a search warrant, the issuing magistrate's task is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit, there is a fair probability that evidence of a crime will be found in a particular place. *State v. Spillers*, 847 N.E.2d 949 (Ind. 2006). The reviewing court's duty is to determine whether the issuing magistrate had a "substantial basis" for concluding that probable cause existed. *Id.* at 953. A substantial basis requires the reviewing court, with significant deference to the magistrate's determination, to focus on whether reasonable inferences drawn from the totality of the evidence support the finding of probable cause. *State v. Spillers*, 847 N.E.2d 949. A "reviewing court" for this purpose includes both the trial court ruling on a suppression motion and an appellate court reviewing that decision. *Id.* at 953. Although we review de novo the trial court's substantial-basis determination, we afford the magistrate's determination significant deference as we focus on whether reasonable inferences drawn from the totality of the evidence support that determination. *State v. Spillers*, 847 N.E.2d 949. In determining whether an affidavit provided probable cause for the issuance of a search warrant, doubtful cases are to be resolved in favor of

upholding the warrant. *Rios v. State*, 762 N.E.2d 153 (Ind. Ct. App. 2002). Additionally, we will not invalidate a warrant by interpreting probable cause affidavits in a hypertechnical, rather than a commonsense, manner. *Id.*

We first address Mehring's argument that the trial court erred when it found that the information upon which the search warrant was based was not stale. "Time can be a critical requirement in determining probable cause." *Williams v. State*, 426 N.E.2d 662, 667 (Ind. 1981). "It is a fundamental principle of search and seizure law that the information given to the magistrate or judge in the application for a search warrant must be timely." *Breitweiser v. State*, 704 N.E.2d at 499 (citation omitted). The general rule is that stale information cannot support a finding of probable cause. *Seeley v. State*, 782 N.E.2d 1052 (Ind. Ct. App. 2003), *trans. denied, cert. denied*, 540 U.S. 1020. Rather, it only gives rise to a mere suspicion, especially where the items to be obtained in the search are easily concealed and moved. *Id.* The exact moment when information becomes stale cannot be precisely determined. *Id.* Although the age of the information supporting an application for a warrant can be a critical factor when determining the existence of probable cause, our courts have not established a bright-line rule regarding the amount of time that may elapse between obtaining the facts upon which the search warrant is based and the issuance of the warrant. *Breitweiser v. State*, 704 N.E.2d 496 (citing *Moran v. State*, 644 N.E.2d 536 (Ind. 1994)). "[P]robable cause is not determined by merely counting the number of days between the occurrence of the facts relied upon and the warrant's issuance." *Id.* at 499. Instead, whether the information is tainted by

staleness must be determined by the facts and circumstances of each particular case. *Breitweiser v. State*, 704 N.E.2d 496.

Mehring contends that the ten-month, nineteen-day delay between when the FBI agent downloaded the child pornography images from Mehring's IP address (May 4, 2005) to when IPD Detective Spivey applied for the search warrant (March 23, 2006) rendered the information stale for the search warrant.

The State acknowledges that the age of the information supporting an application for a search warrant is a critical factor in determining the existence of probable cause but argues that the nature of the items sought, along with the information from Detective Spivey regarding the preservation habits of people who have child pornography, show that the search warrant information was not stale.

> Digital pornography is not like drugs or untaxed cigarettes which are more likely to be consumed on receipt and vanish after a short period of time. Unlike stolen property, for example, digitized pornography can be distributed without destroying or physically transferring it to someone else. It can be shared over peer-to-peer networks repeatedly without vanishing, and resides on electronic media such as compact discs or hard drives. As Detective Spivey's affidavit indicates, child pornography is durable, difficult to obtain, and illegal.

Appellee's Brief at 8. In support of its argument that the search warrant was not stale, the State cites to some federal cases, including the two cases relied upon by the trial court—*United States v. Newsom*, 402 F.3d 780 (7th Cir. 2005) and *United States v. Lacy*, 119 F.3d 742 (9th Cir. 1997), *cert. denied*, 523 U.S. 1101 (1998).

In *Lacy*, the court explained that the lapse of a substantial amount of time is not the controlling factor in a determination of staleness and that such an evaluation must

also include the particular facts of the case as well as the nature of the criminal activity and the property sought. *United States v. Lacy*, 119 F.3d 742. The affiant applying for a search warrant of Lacy's apartment explained, based on her training and experience, that collectors and distributors of pornography value their sexually explicit material, rarely dispose of it, and store it in a secure place—typically, their homes—for long periods of time. *United States v. Lacy*, 119 F.3d 742. The *Lacy* court, while "unwilling to assume that collectors of child pornography keep their materials indefinitely," held that a ten-month span between the initial discovery of information that the defendant had child pornography on his computer and the issuance of the search warrant did not render the information stale where the affidavit "provided ample reason to believe the items sought were still in Lacy's apartment" even ten months later. *United States v. Lacy*, 119 F.3d at 746.

In *Newsom*, the court also noted that the age of information is only one factor in the consideration of whether probable cause exists and that "if other factors indicate that the information is reliable the magistrate should not hesitate to issue the warrant." *United States v. Newsom*, 402 F.3d at 783 (citation omitted). The affidavit provided information that pornographic images of very young children had been discovered on the defendant's computer one year earlier and a hidden camera video of the defendant's ex-girlfriend's daughter coming out of the shower had been "recently" discovered, and the affidavit also explained that computers have ample storage space for hundreds or thousands of images. *Id.* The *Newsom* court explained that "[i]nformation a year old is not necessarily stale as a matter of law, especially where child pornography is concerned" and held that it was

reasonable to conclude that probable cause existed to believe that the defendant had child pornography in his home. *Id.*

Like these federal cases, Indiana cases that have addressed the alleged staleness of facts shown as probable cause in an application for a search warrant have also focused on more than just the age of the information supporting an application for a search warrant. When making a staleness determination, our Indiana Supreme Court and our court have also looked at the nature of the crime, the nature and type of evidence seized or sought, and even a police affiant's opinion, based on his training and experience, regarding the nature of the evidence sought. *See, e.g.*, *Moran v. State*, 644 N.E.2d 536 (holding that the three-month interval between a trash search and the issuance of warrant did not make the warrant information stale where the facts contained in the affidavit permitted the conclusion that the nature of the crime was an ongoing marijuana growing operation and the nature of evidence (beds and other growing equipment) would not be easily moved or exhausted); *Williams v. State*, 426 N.E.2d 662, 667 (holding that the sixty-seven-day interval between the crime and the issuance of the search warrant did not render the information stale where the nature of evidence—burned remnants of a purse and its contents of ashes and sludge—had an "innocent appearance and no utility" and there was a "substantial probability that refuse of this nature [would] not be removed from the site of the burning"); *Allen v. State*, 798 N.E.2d 490 (Ind. Ct. App. 2003) (holding that the information upon which the warrant was based was not stale because the type of evidence sought (weapons) were the type of property that a person reasonably could be expected to keep for over one month); *Seeley v. State*, 782 N.E.2d at 1061 (noting that the passing of

one month between the alleged conduct and the issuance of the warrant was not dispositive of a determination of staleness and explaining that based on the type of evidence sought (mirrors with drug residue and not the actual drugs), it was "logical to conclude" that the mirrors could still contain drug residue and that they could still be located in the premises sought to be searched); *Breitweiser v. State*, 704 N.E.2d 496 (explaining that the character of the criminal activity under investigation is an important factor to consider when determining whether evidence of a crime is still in a particular place); *McGrew v. State*, 673 N.E.2d 787, 793 (Ind. Ct. App. 1996), (holding that the eighty-one-day duration between the information obtained upon which a warrant was based and the issuance of the warrant did not render the warrant stale because the nature of the evidence seized, i.e., a dildo, was "the type of property which [the defendant] could reasonably be expected to keep"), *aff'd in relevant part, vacated in part on other grounds* by 682 N.E.2d 1289 (Ind. 1997); *Foster v. State*, 633 N.E.2d 337, 345 (Ind. Ct. App. 1994) (holding that the twenty-eight-day interval between the crime and the issuance of the search warrant did not render information stale because—unlike controlled substances, which are expected to be consumed or distributed—the type of items seized were in part "innocuous" (child's car seat, fur garment, and adhesive tape) and in part the sort of property that a defendant "reasonably could be expected to keep" (charge card, handgun, and ammunition)), *trans. denied*; *Bigler v. State*, 602 N.E.2d 509 (Ind. Ct. App. 1992) (explaining that, despite the fact that the last known act of amphetamine distribution had occurred twenty-one days before the officers sought the warrant, the element of time loses significance and need not weigh heavily in the determination of

probable cause for the issuance of the search warrant where the facts alleged in the probable cause affidavit established an ongoing amphetamine dealing operation lasting at least two years; the officers sought the warrant to search for evidence that would prove that distribution of amphetamines had been or was being committed (such as business and financial records, proceeds, and paraphernalia) as opposed to a search for amphetamines, which are easily moved or destroyed; and the affidavit contained the opinion of the detective, based on his experience as a narcotics investigator, that the type of evidence sought was commonly found in a drug dealer's residence), *trans. denied*.

With this caselaw to guide us, we conclude the information in this case was not stale. While a ten-month lapse between the initial discovery of child pornography on Mehring's IP address and the application for the search warrant is, on its face, cause for concern, this is just one factor in our determination of staleness. Considering the nature of the crime (possession of child pornography, which is a crime commonly committed in secret and the evidence of which is likely to be kept in a safe and private place like a home) and the nature and type of evidence sought (digital or computer images saved to a computer hard drive or to other types of digital media that can be shared yet still retained), in conjunction with the information provided by Detective Spivey—based on his training and experience as a vice detective—regarding the retention habits of people having child pornography, we agree with the trial court that the ten-month time period did not render the information stale.

We next address Mehring's contention that the search warrant was not supported by probable cause because there were no facts from which the magistrate could conclude

that the Brian Mehring at the 896 Blake Street address was the same Brian Mehring who lived at the 732 Lockfield Court address or that Mehring still had the computer or the images downloaded by the FBI agent in May 2005 on his computer when the warrant was issued and executed in March 2006.

First, we disagree with Mehring's suggestion that the information provided in the affidavit was so lacking that the magistrate was left to guess whether he was the same Brian Mehring. Here, the affidavit provided that: the child pornography images downloaded by the FBI agent on May 4, 2005, came from the IP address belonging to Brian Mehring, who lived at 732 Lockfield Court, Apartment B in Indianapolis; the Lockfield apartment was found to be vacant when visited by Detective Spivey; further police investigation revealed that Mehring had relocated to 896 Blake Street, Apartment B in the same Lockfield Gardens Apartment Complex; and police verified that Mehring lived at the 896 Blake Street address by seeing his name listed on the mailbox and by going to his door and identifying him by name and date of birth. From this information, it was reasonable for the magistrate to conclude that the Brian Mehring at the 896 Blake Street address was the same Brian Mehring who lived at the 732 Lockfield Court address.

We also reject Mehring's argument that probable cause was lacking because the affidavit did not specifically show that Mehring still had the computer or the images downloaded by the FBI agent in May 2005 on his computer when the warrant was issued and executed in March 2006. We note that probable cause does not require a demonstration that contraband will be found on the premises to be searched; it requires only a fair probability of criminal activity. *Rios v. State*, 762 N.E.2d 153. Furthermore,

the issuing magistrate is to make common-sense decisions and reasonable inferences from the facts set forth in the affidavit. Here, the affidavit provided that Mehring provided child pornography images from his IP address to a file sharing network when he lived in the Lockfield apartment address and that he moved to the Blake Street apartment address. In the affidavit, Detective Spivey stated that it was probable that Mehring had his computer with him at his new address. Furthermore, given the nature and portability of computers, the issuing magistrate could have made a reasonable inference that Mehring took his computer with him when he moved.

Given the information contained in the affidavit, the nature of the crime being investigated, the nature of the items being sought, and the normal and common sense inferences regarding where one might keep such items, we agree with the trial court that the issuing magistrate had a substantial basis for concluding that probable cause existed and that there was a fair probability that evidence of child pornography was probably present in Mehring's residence. Therefore, the trial court did not err when it denied Mehring's motion to suppress.

Mehring contends, however, the search of his apartment pursuant to the search warrant was in violation of article 1, section 11 of the Indiana Constitution because he has greater protection under the Indiana Constitution. Article 1, section 11 provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search or seizure, shall not be violated; and no warrant shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the person or thing to be seized.

Although the language of article 1, section 11 largely tracks the language of the Fourth Amendment, Indiana has adopted a different analysis for claims brought under article 1, section 11. *Litchfield v. State*, 824 N.E.2d 356. Under Indiana's analysis, the validity of a search by the government turns on an evaluation of the reasonableness of the officer's conduct given the totality of the circumstances.[4] *Id.* (citing *Moran v. State*, 644 N.E.2d 536). "[T]he reasonableness of the official behavior must always be the focus of our state constitutional analysis" and "[t]he state standard of reasonableness frequently requires that police action occur only with a judicial sanction." *Moran v. State*, 644 N.E.2d at 539.

As noted above, the totality of the circumstances—including, the information contained in the affidavit, the nature of the crime, the nature of the items being sought, and the normal and common sense inferences regarding where one might keep such items—established a substantial basis to believe that there was a fair probability that evidence of child pornography would be found in Mehring's apartment. Thus, upon review of the totality of the circumstances, the search of Mehring's apartment pursuant to the search warrant was reasonable and did not violate article 1, section 11. *See, e.g.*, *Moran v. State*, 644 N.E.2d 536 (holding that there was probable cause for the issuance

[4] Mehring references the three factors discussed in *Litchfield*—degree of concern that a violation has occurred; degree of intrusion upon a citizen's ordinary activities; and extent of law enforcement needs—as applicable to a determination of the staleness issue and whether there was probable cause for the issuance of the search warrant. Because the search discussed in *Litchfield* was a warrantless search and the three factors are relevant to a determination of reasonableness when a warrantless search occurs, we do not agree that they are applicable under the facts of this case.

of a search warrant and that the search of the defendant's residence pursuant to the search warrant was reasonable under the Indiana Constitution).

Ruling affirmed.

ROBB, J., concurs.

MATHIAS, J., dissents with separate opinion.

IN THE
COURT OF APPEALS OF INDIANA

BRIAN MEHRING,	)	
	)	
Appellant-Defendant,	)	
	)	
vs.	)	No. 49A05-0706-CR-337
	)	
STATE OF INDIANA,	)	
	)	
Appellee.	)	

Mathias, J., dissenting

I respectfully dissent.

I am very sensitive to the tragedy of child pornography, but eleven months is a very long time, especially when one of the most important criteria for the issuance of a search warrant is the accuracy of the facts alleged. Such accuracy usually has an inverse relationship to the age of the facts alleged. This is precisely why stale information cannot and should not support the finding of probable cause. See Seeley, 782 N.E.2d at 1060. Instead, such stale information gives rise only to a mere suspicion, "especially when the items to be obtained in the search are easily concealed and moved." Id. It is hard to imagine something that can be more easily concealed, moved, or even destroyed than a digital image. Indeed, such images are a mouse-click away from being moved or deleted.

If deleted with today's computer utility software, such files may well not be recoverable, even with the best forensic software and techniques.[5]

I would also note that in the Indiana cases cited by the majority, the staleness of the information did not even approach eleven months. See Allen, 798 N.E.2d at 498 (almost two months); Seeley, 782 N.E.2d 1061 (one month); McGrew, 673 N.E.2d at 793 (eighty-one days); Moran, 644 N.E.2d at 541-42 (three months); Foster, 633 N.E.2d at 345 (twenty-eight days); Bigler, 602 N.E.2d at 516 (twenty-one days); Williams, 426 N.E.2d at 667 (sixty-seven days).

Moreover, the facts in Newsom, one of the federal cases cited by the majority, are readily distinguishable. In addressing the sufficiency of the information supporting the search warrant in that case, the Newsom court specifically noted that, in addition to having seen child pornography on the defendant's computer over a year earlier, the girlfriend had "*recently* discovered videos of her daughter." 402 F.3d at 783 (emphasis added). Unlike Newsom, this is not the case where the police have *recently* come into possession of information of a crime which may have occurred some time ago. Instead, the police here had information that Mehring may have possessed child pornography on his computer over ten months ago. Without more, this extremely stale information cannot and should not be adequate for a finding of probable cause.

[5] See, e.g., http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx ("The only way to ensure that deleted files . . . are safe from recovery is to use a secure delete application. Secure delete applications overwrite a deleted file's on-disk data using techniques that are shown to make disk data unrecoverable, even using recovery technology that can read patterns in magnetic media that reveal weakly deleted files.").

To support their conclusion, the majority relies upon Detective Spivey's opinion that those who view child pornography tend to store such illegal information for long periods of time. This opinion is accepted as factual despite not being subject to cross-examination or being corroborated by any supporting professional article on the topic, which, if the opinion is accurate, should not have been difficult to obtain during the almost eleven-month interim.

I do not believe the opinion of the Ninth Circuit Court of Appeals in Lacy is persuasive on this issue. The Lacy court simply relied upon a similarly unsupported claim by a customs agent that collectors of child pornography tend to retain such materials for long periods of time. 119 F.3d at 746. Just because this allegation is repeated does not make it true.[6] Under the majority's reasoning, both the durability of digital images and the alleged tendency of pedophiles to hoard and preserve such images would justify a search warrant based upon information that was not only several months old, but several years old.[7]

---

[6] This is not to say that I would be surprised if this proposition were borne out by actual evidence. It is also noteworthy that this allegation shows up in substantially similar language in law enforcement probable cause affidavits in many cases, both state and federal. See e.g., United States v. Zimmerman, 277 F.3d 426, 433 (3d Cir. 2002); United States v. Harvey, 2 F.3d 1318, 1323 (3d Cir. 1993); United States v. Koelling, 992 F.2d 817, 819 (8th Cir. 1993); United States v. Rabe, 848 F.2d 994, 996 (9th Cir. 1988); People v. Nicholls, 71 Cal.Rptr.3d 621, 624 (Cal. Ct. App. 2008); Commonwealth. v. Gomolekoff, 910 A.2d 710, 714 (Pa. Super. Ct. 2006); Taylor v. State, 54 S.W.3d 21, 23 (Tex. App. 2001).

[7] For example, too many homeowners have "open" wireless internet connections which do not require a password to use. Any houseguest, neighbor, or passerby with a wireless internet device could download child pornography through that open connection unbeknownst to the homeowner. Under the majority's holding, the homeowner would then become subject to searches of his or her home and computer months or even years later, without any information supporting the search warrant other than the fact that, some time ago, someone used the homeowner's internet connection to download illegal materials. While such facts may be a strong reason to use a closed, password-protected wireless internet connection, I do not think they should justify the issuance of a search warrant.

Finally, nowhere did any investigating authority explain to the trial court or to this court on appeal why the extremely broad electronic eavesdropping authority available to law enforcement today was never used during the intervening eleven months before the search warrant was issued. Such eavesdropping on Mehring's current IP address could well have disclosed the fresh and accurate information that search warrants are supposed to be based and depend upon. Cf. Newsom, 402 F.3d at 782. Even a simple LimeWire search, which was the genesis of the investigation of Mehring almost eleven months earlier, could have revealed whether images of child pornography had more recently been available from the IP address of Mehring's computer. This is not an onerous burden to place upon law enforcement before authorizing the police to enter a citizen's home and search her or his computer.

In short, I do not believe that the information provided in the probable cause affidavit supported the trial court's issuance of a search warrant. I would therefore reverse the trial court's decision and grant Mehring's motion to suppress.